Relazione tecnica

per la fornitura di "Servizi di Cloud Computing"

CONSIP SPC CLOUD LOTTO1

Conservazione Digitale – Cloud Enabling

Sommario

1 Conservazione digitale

La conservazione a norma è finalizzata all'estensione e al mantenimento della validità dei documenti conservati, garantendone nel tempo la fruibilità, l'inalterabilità e la validità ai fini legali. Il sistema di conservazione a norma riceve i pacchetti di versamento generati dai sistemi dell'Amministrazione contraente e produce pacchetti di archivia-zione e di distribuzione conformi a tutti i requisiti posti dalla normativa per l'esibizione dei documenti informatici, arricchendo le informazioni che accompagnano i dati conservati e tracciando tutte le attività che li riguardano.

1.1 L'organizzazione del servizio

Il servizio vede, come attori, gli "utenti produttori" dell'Amministrazione, coloro che producono i documenti da conservare e che generano e inviano i pacchetti di versamento (SIP) al sistema di conservazione;gli "utenti visori", coloro che sono abilitati ad esibire i documenti conservati a fini legali, e che a questo scopo richiedono la generazione di pacchetti di distribuzione (DIP). Il processo è gestito dall'azienda del Raggruppamento qualificata come conservatore accreditato, che trasforma i pacchetti di versamento in pacchetti di archiviazione (AIP).

Il servizio di conservazione a norma rispetta la normativa espressa nel Decreto del Presidente del Consiglio dei Ministri del 3 Dicembre 2013, pubblicato in Gazzetta Ufficiale n.59 del 12-3-2014 - Suppl. Ordinario n. 20 [NORM]. Nella stessa normativa sono indicati gli standard da adottare per la conservazione e la gestione archivistica dei dati digitali.

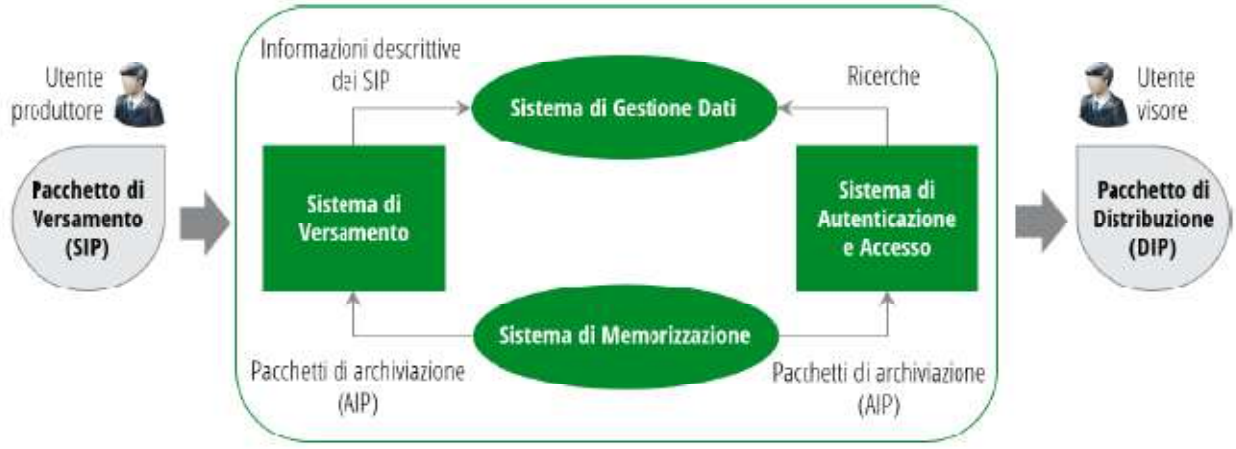


Figura – Processo di conservazione a norma

Il servizio risponde a tutti i requisiti di gara, ed è pienamente conforme alla normativa vigente e ai migliori riferimenti tecnici e di prassi, quali ad esempio le linee guida dell'AgID. In entrambe le versioni proposte, il servizio è presente sul mercato da molti anni: viene continuamente adeguato all'evoluzione normativa e adotta le migliori tecnologie disponibili per garantire i massimi livelli di servizio.

Il servizio può essere fruito in tre modalità:

- manuale – basata su interfaccia utente web;
- attraverso scambio di flussi mediante FTP;
- in modalità integrata tramite web service con i sistemi dell'Amministrazione;

ed è in grado di trattare documenti di rilevanza fiscale, quali fatture, libri e registri contabili; documenti relativi al personale; delibere e determine; contratti. È possibile definire nuove classi documentali "custom"

per rispondere ad esigenze specifiche delle Amministrazioni. In sede di predisposizione del Piano dei Fabbisogni ciascuna Amministrazione dovrà indicare:

- la quantità di spazio di conservazione richiesto;
- quali modalità attivare (una o più di una);
- quali tipologie di documenti trattare (una o più di una);
- quali utenti utilizzeranno il servizio, distinguendo fra "produttori" e "visori";

in modo da consentire al Raggruppamento una corretta configurazione del servizio.

Il processo si articola in tre fasi principali: conservazione, verifica periodica di integrità, esibizione.

Le fasi del processo di conservazione si possono così riassumere:

- l'utente invia (via portale web e/o web service e/o SFTP) i lotti di documenti con i relativi metadati;
- i lotti di documenti sono accettati e viene fornito un identificativo univoco di lavorazione, se è superata positivamente la fase di validazione; in caso contrario si emette una ricevuta di scarto, con il dettaglio dell'errore, e viene eventualmente sospeso il lotto (es., per documenti a valenza tributaria);
- i lotti validati vengono caricati sul sistema di gestione documentale;
- per ogni pacchetto viene creato il file indice;
- nel caso siano verificati i criteri di chiusura di ciascun pacchetto si attiva la richiesta di marca e firma alla Certification Authority;
- il sistema di Certification Authority restituisce il file indice con la marca e la firma;
- il sistema di conservazione associa la marca e la firma al pacchetto di archiviazione;
- il pacchetto di archiviazione viene chiuso e reso disponibile per l'esibizione a norma sotto forma di pacchetto di distribuzione.

I documenti vengono conservati con garanzia di leggibilità nel tempo, rispettando le norme in vigore per quanto attiene ai formati ammessi.

La verifica di integrità, già effettuata in fase di validazione, verrà ripetuta periodicamente, al fine di garantire l'integrità e l'inalterabilità del documento nel tempo, confrontando l'impronta attuale con quella contenuta nell'Indice di conservazione e fornita a suo tempo dall'utente produttore. Tale funzionalità assolve i requisiti di verifica periodica della leggibilità dei documenti, come enunciati dalla normativa vigente.

Le funzionalità di esibizione, infine, consentono all'utente visore di:

- ricercare uno o più documenti con opportuni criteri (es. data caricamento, stato, metadati), fino ad un massimo di oc-corrènze (configurabile dall'utente);
- vedere lo stato dei documenti ricercati;
- consultare uno o più documenti fra quelli ricercati;
- visualizzare i pacchetti di archiviazione per l'esibizione a norma con le opportune verifiche.

In fase di esibizione verranno fornite tutte le informazioni utili alla verifica, con specifico riferimento alla validità della firma e della marca temporale.

Attraverso la console di gestione del servizio, il Referente tecnico dell'Amministrazione è in grado di:

- assegnare agli utenti i profili (produttore o visore);
- attivare/disattivare una classe, attivare/disattivare i controlli sugli indici; la creazione di una nuova classe può avvenire sia ex-novo sia partendo da una già esistente (copia);

- monitorare il servizio, visualizzando sia lo spazio consumato e il residuo rispetto a quanto contrattualizzato, sia le richieste e le operazioni svolte insieme ai rispettivi stati di lavorazione: ad esempio, è possibile visualizzare il numero di documenti in attesa di essere aggiunti ai pacchetti di archiviazione, il numero di documenti da conservare, il numero di documenti che sono già stati conservati, ecc.; sono presenti notifiche che segnalano eventuali scadenze dei certificati.

Nel caso l'Amministrazione utilizzi già processi di conservazione digi-tale, a piattaforma è in grado di importare dati conservati in conformità alla norma vigente (DPCM 3/12/2013) o alla deliberazione CNIPA n. 11/2004. La verifica di tali conformità è preventiva rispetto all'accettazione dei dati conservati da migrare.

1.2 Servizio L1.S4.4 – Conservazione digitale

Il servizio "SaaS – Conservazione digitale" permette alle Amministrazioni di usufruire di un servizio applicativo fornito in modalità "As a Service" che metta a disposizione degli utenti le principali funzionalità di conservazione digitale. Il servizio di conservazione consente alle Amministrazioni, dal momento della presa in carico e per tutto il periodo prescritto dalla norma, fino all'eventuale scarto, la conservazione dei documenti, dei fascicoli informatici e dei relativi metadati associati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità e garantendone altresì l'accesso indipendentemente dalle evoluzioni tecnologiche.

Il servizio è erogato in ottemperanza alla normativa vigente, con particolare riferimento alle regole tecniche indicate nel DPCM 2013/03/12 "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005" e successiva circolare "Circolare 10 aprile 2014, n. 65 - Accreditamento e vigilanza conservatori".

La normativa vigente prevede inoltre che, per l'espletamento del processo di conservazione, il Fornitore debba essere accreditato attraverso un processo di accreditamento secondo quanto riportato nella Circolare dell'Agenzia per l'Italia Digitale del 10 aprile 2014, n. 65 "Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82" pubblicata nella Gazzetta Ufficiale n.89 del 16 aprile 2014. Il Fornitore, nel caso ne fosse sprovvisto, deve ottenere l'accreditamento entro novanta giorni dalla data di stipula del Contratto Quadro e mantenerlo per l'intera durata del Contratto Quadro. Il servizio non potrà essere erogato fino all'ottenimento dell'accreditamento. In caso di mancato accreditamento, ovvero di revoca e/o sospensione dell'accreditamento, è prevista la risoluzione del Contratto Quadro per la parte inerente il servizio di conservazione digitale.

TIM, tramite l'azienda consociata Trust Technology, si è impegnata nella conservazione dei documenti trasferiti e ne ha assunto la funzione di responsabile della conservazione ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione.

TIM, tramite l'azienda consociata Trust Technology, ha messo a disposizione dell'Amministrazione il Manuale di conservazione, redatto nel rispetto della normativa vigente sulla tutela degli archivi e dei singoli documenti. Il servizio di conservazione e di restituzione dei documenti a fini di accesso e/o di ricerca è erogato in base al suddetto Manuale di conservazione.

TIM è impegnata nel costante adeguamento del servizio di conservazione alle eventuali future modifiche normative.

Il servizio non necessita l'integrazione con altre tipologie di risorse virtuali (risorse base, macchine virtuali e componenti di rete).

Tale servizio è reso disponibile a partire dalla acquisizione di licenze di utilizzo dei servizi applicativi per singoli utenti o di spazio storage/volumi di documenti oggetto di conservazione a norma, con successiva possibilità di espansione o riduzione di tale numerosità di licenze/risorse, in completa autonomia, a seconda delle diverse esigenze dell'Amministrazione.

Per il servizio non è previsto il rinnovo automatico delle licenze di utilizzo.

Tale servizio non necessita l'integrazione con altre tipologie di risorse virtuali (risorse base, macchine virtuali e componenti di rete).

TIM, nell'ambito del servizio "SaaS - Conservazione digitale", garantisce la disponibilità per l'Amministrazione di un servizio applicativo che garantisca i requisiti minimi indicati nel DPCM 2014/03/12. Inoltre, dal punto di vista funzionale, tale servizio garantisce la disponibilità delle seguenti funzionalità base:

- il servizio è disponibile attraverso un'interfaccia web-based che può pertanto essere acceduta tramite browser ed è reso disponibile alle applicazioni che richiedono la conservazione attraverso web services;
- adozione di un formato elettronico di conservazione dei dati e dei supporti che garantisce la non alterabilità e autenticità e che ne preserva l'integrità per tutto il periodo di conservazione secondo la normativa vigente;
- funzionalità di indicizzazione e fascicolazione dei documenti, di ricerca avanzata ed estrazione dal sistema di conservazione secondo la normativa vigente;
- funzionalità di archiviazione, classificazione e catalogazione di flussi e documenti digitali di diversi formati (ad es. documento proveniente da procedure gestionali, immagine, testo, disegno, file, fax, suono, video, messaggio);
- funzionalità per la conversione di formato dei documenti nel formato definito di conservazione;
- disponibilità di una reportistica completa che consenta di monitorare e di verificare la situazione dei documenti, dei pacchetti di versamento, archiviazione e distribuzione;
- tracciamento e memorizzazione di tutte le operazioni effettuate dal Responsabile della Conservazione;

Dal punto di vista tecnologico, il servizio prevede:

- interoperabilità con i principali formati di documenti digitali più utilizzati in ambito produttività individuale, imaging (i.e. almeno .doc, .docx, .pdf, .rtf, .png, .jpeg …);
- compatibilità con i principali e più diffusi dispositivi Mobile.

Il servizio "SaaS - Conservazione digitale" è erogato in modalità "continuativa" di tipo "as-a-Service".

I servizi di conservazione riguardano i documenti di RIS/PAC, fatture, amministrativi, atti e delibere. Essi verranno erogati per gestire una mole di dati pari a 8,7 TB per 12 mesi.

1.3 Il versamento dei documenti in conservazione

L' Archiving Gateway (ArG) è il software che predispone i pacchetti di versamento ed espone servizi differenti per la raccolta dei documenti da archiviare.

L'acquisizione dei documenti avviene mediante l'utilizzo di "Adapter". Nel paragrafo successivo sono riportati i principali adapter implementati.

Successivamente l'acquisizione dei documenti, l'appliance "Volumizer", installato sull'ArG, predispone i pacchetti di versamento da sottoporre alla procedura di consolidamento.

Il pacchetto di versamento viene generato secondo lo standard UNI SinCRO e personalizzato secondo le specifiche esigenze dell'Ente.

L'Ente può scegliere se creare pacchetti di versamento associando documenti "simili" o semplicemente in ordine di produzione: per documenti simili si intende qualsiasi tipologia di documento (DICOM o pdf) con un particolare valore di un determinato campo (stessa provenienza, stesso medico, stessa data…). I pacchetti di versamento saranno chiusi in base alla dimensione totale raggiunta o allo scadere dell'arco temporale massimo definito.

Di fondamentale importanza per la creazione dei pacchetti, tematica ampiamente riportata nella fase di predisposizione del manuale della conservazione, è la gestione delle eccezioni.

Le eccezioni sono anomalie definite riscontrate nei documenti da archiviare.

Esempi tipici di anomalie sono, ad esempio:

- Firma non valida del medico repertante (scaduta, revocata…);
- Documento corrotto;
- Campi, definiti come obbligatori, non compilati (nome e cognome paziente, data di produzione esame…).

I documenti per i quali viene evidenziata un'eccezione non vengono portati in conservazione e riportati tra i documenti scartati.

L'Appliance "Trasfer", infine, provvede ad inoltrare il pacchetto di versamento verso il Data Center utilizzando canali sicuri.

Di seguito si riporta l'elenco degli adapter installabili sul sistema ArG:

a) Adapter DICOM: consente l'acquisizione di immagini DICOM utilizzando procedure standard Storage/Storage Commitment e Query/Retrieve DICOM 3.0;
b) Adapter Hl7: consente l'acquisizione di documenti utilizzando il messaggio standard Hl7 (ver. 2.6 o successive) "MDM T10";
c) Adapter Vista: questo adapter consente di acquisire documenti e metadati direttamente da apposite viste. L'Adapter può acquisire documenti da DBMS "Oracle", "MySql", PostGres", "MS SQL Server". Il file fisico può essere memorizzato sia in campo BLOB del DB che sul filesystem.
d) Adapter FTP: questo adapter acquisisce documenti e metadati da una specifica cartella FTP. Per ciascuna sorgente documentale viene generata una folder FTP che conterrà il file fisico ed un file XML standard per l'acquisizione dei metadati.
e) Adapter FileSystem: consente di acquisire i documenti ed i metadati o un intero pacchetto di versamento già costituito, direttamente da un file system condiviso.
f) Adapter WS: consente di acquisire ed esibire i documenti di un pacchetto di versamento mediante tecnologia WEB J2EE utilizzando servizi di interoperabilità poggiati su architettura REST.

2 Servizi di Cloud Enabling

L'attuale architettura del data center dell'AORN Santobono si configura come una piattaforma di Cloud Computing, ibrida, costituita da una componente di Cloud Privato, installata presso il CED dell'Amministrazione e caratterizzata da una soluzione in business continuity (sito primario presso il CED di via Mario Fiore; sito BC presso il CED di via Croce Rossa) ed una componente di Cloud Pubblico, in cui è installato il sito di disaster recovery, presso l'IDC di SPC Cloud (TIM Acilia).

Tale scelta architetturale, dettata dalle particolari esigenze applicative dell'AORN, è in evoluzione. Dopo un periodo di assestamento, l'AORN procederà con la progressiva migrazione delle applicazioni non critiche verso il Cloud Pubblico, in modo raggiungere i livelli di servizio dettati dall'Agenda Digitale.

Ciò comporta la disponibilità di servizi professionali che garantiscano il processo di migrazione al Cloud Pubblico. Questi servizi sono fruibili tramite la convenzione CONSIP SPC Cloud, servizi di Cloud Enabling.

2.1 Supporto al Cloud Ibrido

Il servizio, erogato da diverse figure professionali, si basa su una metodologia di analisi e supporto per fornire all'AORN gli elementi decisionali per l'adozione di servizi Cloud, i diversi tipi di attività di supporto operativo e la metodologia progettuale per le migrazioni "Physical-to-Virtual".

Gli interventi di Cloud Enabling avranno l'obiettivo di accompagnare l'AORN nell'adozione dei servizi Cloud previsti.

Con il servizio Cloud Enabling verranno trasferite all'AORN le conoscenze necessarie per l'utilizzo proficuo ed efficiente dei servizi, in particolare relative a:

- il Cloud Computing: aspetti organizzativi, funzionali, tecnologici;
- funzioni del Portale di Governo e Gestione della Fornitura e componenti associate;
- Servizi IaaS e PaaS:
    - risorse virtuali di infrastruttura e solution stack;
    - funzioni del Portale dei Servizi di Cloud Computing;
    - utilizzo delle risorse IaaS/PaaS nell'ambiente ICT dell'Amministrazione;
- Servizi SaaS e Backup as a Service:
    - potenzialità dei servizi;
    - modalità d'uso e di amministrazione dei servizi;
    - console di gestione dei servizi.

Quindi si potrà:

- accedere al materiale descrittivo, presente nel sistema documentale della fornitura e disponibile liberamente ai referenti;
- accedere ai tutorial specifici dei servizi SaaS, ove previsti;
- richiedere workshop dedicati, riferiti specificamente all'utilizzo dei servizi, negli aspetti di interesse per l'Amministrazione stessa;
- richiedere tutoring/affiancamento dedicato, erogato on-site da specialisti a supporto dei referenti nella loro attività di amministrazione e gestione dei servizi;
- richiedere supporto operativo erogato on-site da specialisti TIM, in grado di effettuare operazioni di configurazione sulle piattaforme di gestione e/o di fornire supporto ai Referenti nella progettazione degli ambienti virtualizzati;
- richiedere assistenza nella definizione delle politiche di gestione dei servizi – ad esempio, nella definizione delle politi- che di backup.

Il servizio, erogato a consumo, prevede un tetto di giornate tra Capo Progetto e Specialista di Tecnologie/Prodotto, distribuite nel periodo di migrazione al Cloud dell'Amministrazione.

2.2 Supporto alla protezione e prevenzione

Gli stessi servizi di Cloud Enabling sono utilizzati per supportare l'AORN nella definizione di un sistema di protezione e prevenzione dagli attacchi informatici, che tramite la rete Intranet e la rete Internet possono violare i sistemi informatici aziendali.

Gli incidenti di sicurezza stanno crescendo molto rapidamente, sia nel numero sia nella loro efficacia.Questo problema risulta sempre più rilevante, e lo sarà sempre di più in futuro in quanto il processo in atto di Digital Transformation della società è ormai inarrestabile. In particolare, le aziende hanno capito che per rimanere in vita, crescere e diversificare, devono considerare la tecnologia digitale come parte integrante dei propri processi, prodotti e servizi.

Uno dei più importanti elementi costitutivi della trasformazione digitale è la Cybersecurity: mentre risultano chiari i benefici di tale cambiamento, manca la consapevolezza sulle vulnerabilità create da questa trasformazione, vulnerabilità che molto spesso risultano difficili da riconoscere e da intercettare, perché il perimetro non è più solamente tecnologico. C'è quindi la necessità di verificare, monitorare e rendere sicuro l'intero ecosistema, qualcosa che vada al di là della sola tecnologia.

È quindi fondamentale affrontare il tema della sicurezza informatica in tutti i suoi aspetti, focalizzandosi su tutti gli elementi che compongono una azienda: infrastruttura, persone e la cultura aziendale.

In questo contesto di trasformazione digitale l'AORN ha intrapreso un percorso di upgrade dei propri sistemi di sicurezza che sposano i criteri innovativi di approccio alla Cybersecurity. TIM, nell'idea di accompagnare l'AORN in questo percorso, propone una metodologia sviluppata tramite il contributo dei partnerCloud Enabler.

La nostra idea si basa sul cambio di prospettiva, cioè ponendoci dal lato dell'hacker. Per raggiungere i propri obiettivi l'hacker cerca il metodo più efficiente da utilizzare, talvolta sfruttando le falle dell'infrastruttura, sempre più spesso la debolezza del fattore umano.

Noi vogliamo rendere consapevoli le aziende dei rischi che possono scaturire dall'insieme di queste vulnerabilità ed aiutarle a porvi rimedio

People-Centric Security significa mettere le persone al centro di tutta la sfida per la sicurezza, perché sono sempre e comunque le persone ad utilizzare o gestire la tecnologia.

Perché le persone non devono essere viste solamente come parte del problema, esse devono diventare parte della soluzione.

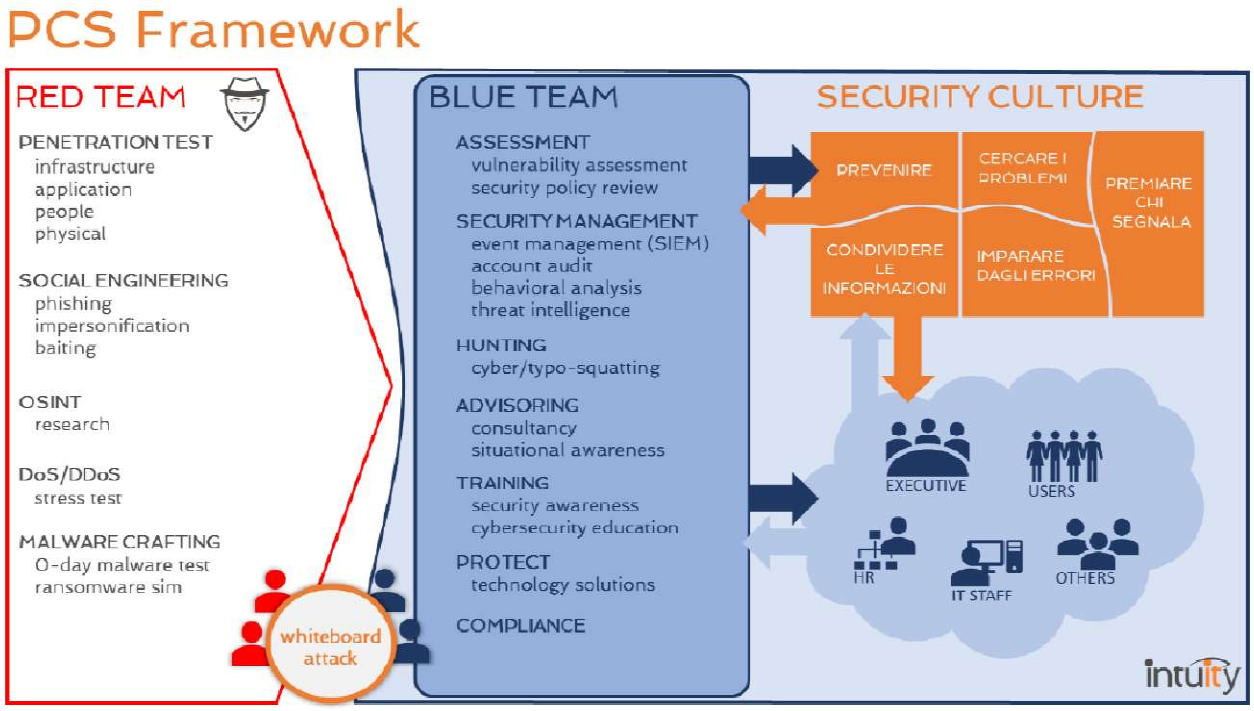
Condividere la stessa Cultura della sicurezza significa avere un modo comune di vedere le cose, di comportarsi e di agire. Significa far muovere l'azienda compatta in una stessa direzione nelle scelte quotidiane legate alla CyberSecurity. Policy, Regolamenti e Compliance sono elementi importanti, ma è fondamentale che questi siano noti, condivisi e assimilati da tutti.

Sono le Persone in un'azienda a prendere le decisioni a compiere azioni. Sono le persone che quotidianamente utilizzano il mezzo tecnologico, accedono ai dati aziendali, pubblicano informazioni sul web. Dare a queste persone la giusta consapevolezza di quali sono le minacce alle quali sono soggetti, loro e l'azienda attraverso di loro, e fornirgli gli strumenti per reagire, significa trasformare una potenziale vulnerabilità in una efficiente difesa.

La sempre crescente complessità delle Infrastrutture informatiche e l'adozione massiva di tecnologie sempre connesse portano con sé anche un aumento preoccupante delle vulnerabilità. Un bug di sistema, una configurazione errata, un documento sensibile divulgato inavvertitamente, una regola di test dimenticata da tempo o un utente con privilegi troppo elevati, sono piccole cose che possono esporre l'azienda a gravi conseguenze.

I servizi offerti consentono di elevare la sicurezza delle aziende in modo efficacie e durevole nel tempo, consentendo di ottimizzare gli investimenti già fatti e quelli futuri.

Conoscere le debolezze presenti che possano comportare un rischio per l'azienda è fondamentale per definire un piano di interventi preciso ed efficacie, focalizzandosi sui rischi primari e soprattutto estendendo il campo di azione anche ad altri ambiti, quali le persone o la cultura aziendale.



La dinamicità con cui cambiano le aziende, il contesto tecnologico in cui queste operano, gli strumenti e i modi in cui questi vengono utilizzati, rende necessario che la sicurezza venga garantita e verificata con continuità in modo da poter rispondere in modo tempestivo ed efficiente al manifestarsi di nuove minacce.

Certificazioni aziendali

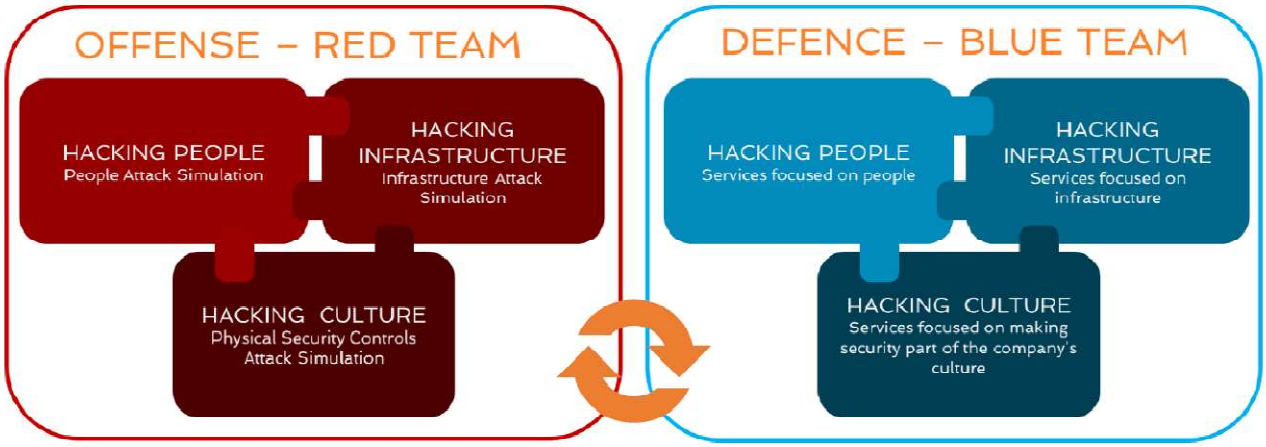
Il nostro è un Laboratorio Qualificato per effettuare attività di VulnerabilityAssessment e Penetration Test conformi con le seguenti circolari Accredia:

- Conservatori a Norma: Circolare Accredia n.5/2017 DC2017SPM0080
- UE 2014_910 eIDAS: Circolare Accredia n.8/2017 DC2017SSV046
- Operatori SPID: Circolare Accredia n.35/2017 DC2016SSV438

OFFENSE vs. DEFENCE: ADAPTIVE SECURITY

L'approccio proposto prevede di attivare un circolo virtuoso dove le informazioni raccolte e le attività d'attacco effettuate dal servizio RED TEAM possano contribuire all'aumento della consapevolezza e della conoscenza del problema (BLUE TEAM), con il conseguente risultato di innalzare il livello di sicurezza aziendale.

Questo continuo processo di attacco vs difesa è il modello da seguire per mettere in atto un sistema difensivo efficace che, coinvolgendo infrastruttura e persone, riesca a "adattarsi" con efficacia ad ogni tipologia di attacco, presente e futuro.



2.2.1 Company Security Culture TransformationProcess

L'obiettivo di questa proposta è quello di definire un percorso che porti l'azienda ad affrontare le tematiche di sicurezza già percepite ed evidenziate dall'azienda, con l'ulteriore obiettivo di far emergere eventuali altrifattori di rischio meno evidenti ma altrettanto significativi.

I servizi proposti hanno si prefiggono i seguenti obbiettivi:

1. Dare evidenza all'Azienda del possibile danno causato da attacchi reali che sfruttano le vulnerabilitàpresenti nell'infrastruttura IT e relativi servizi attivi, quelle relative alle persone e ai controlli disicurezza fisici, sia dall'esterno che dall'interno, in modo da reagire prontamente ad eventuali nuovecriticità rilevate.
2. Misurare il livello di Detection& Reaction nei confronti di attacchi informatici.
3. Misurare e successivamente aumentare la consapevolezza degli utenti aziendali rispetto alproblema del Phishing e della cybersecurity in generale.
4. Rinforzare il livello di sicurezza aziendale reiterando i servizi di simulazione d'attacco e di training alpersonale (rinforzo del messaggio).
5. Supportare l'azienda nella creazione di una Security Culture.

I due servizi (Red e Blue Team) sono stati pensati e sviluppati per affrontare la sicurezza attraverso unapproccio nuovo. La contrapposizione tra le attività di Offensive Security (Red Team) e di Defensive Security(Blue Team) immaginate come un singolo servizio, permette di affrontare il tema della cybersecurity in modo - Phishing - permetterà di "sviluppare" il contenuto di un training che gli utenti aziendali seguiranno in aula una volta condivisi i risultati con i Manager aziendali ed alcuni Key User.

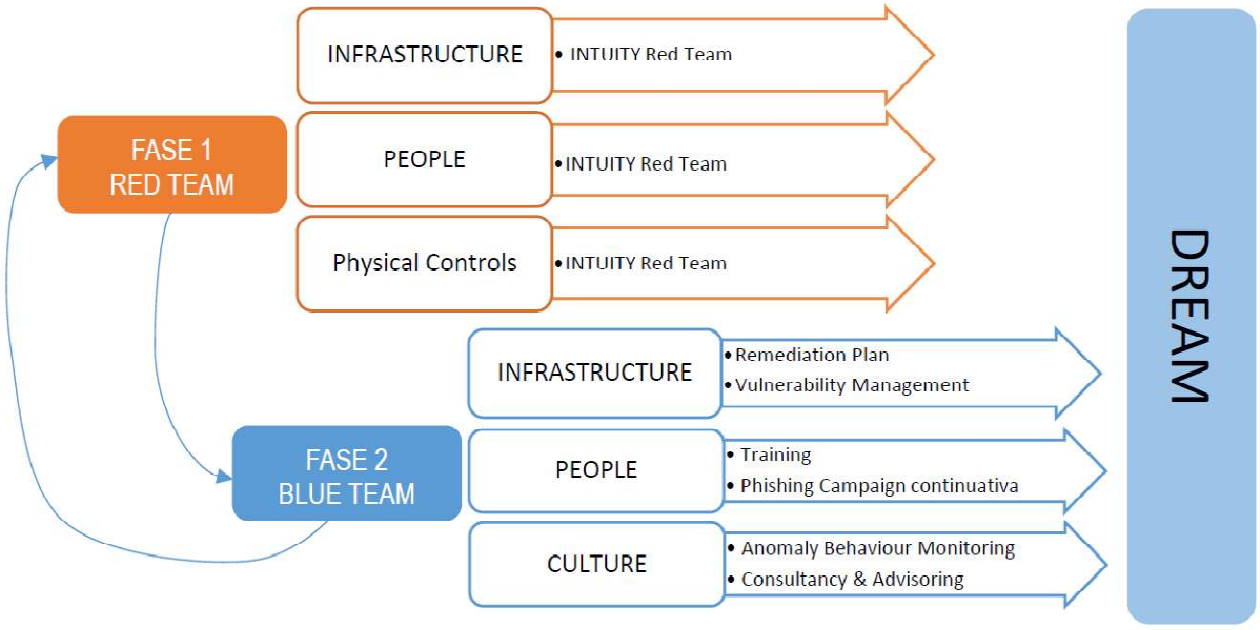
Al termine del servizio RED TEAM, i risultati verranno condivisi con gli stakeholder aziendali al fine di condividere un piano di remediation e le relative azioni di miglioramento.

La seconda fase del percorso proposto prevede di rinforzare il messaggio definito durante il training attraverso una Phishing Campaign prolungata nel tempo. La Phishing Campaign differisce dal Phishing Assessment per il feedback che ogni utente riceverà nel momento in cui cliccherà su un link o tenterà di scaricare un allegato di una mail di Phishing inviata dal sistema di sicurezza. Mentre durante l'attacco Phishing verrà direzionato verso una pagina controllata (es. pagina con errore 404), nella Campaign gli verrà indicato l'errore commesso e proposto una attività di "quick training" online (pochi minuti).

Le competenze ed esperienze dei nostri specialisti che parteciperanno al team di progetto comprendono (vengono elencate le principali):

1. Network Security
2. System Security
3. Application Security
4. Mobile Security
5. Risk identification, Assessment, Evaluation, Response & Monitoring (ISACA CRISC)
6. Social Engineering
   6.1. Technical Methodology
   6.2. Anthropological Methodology
   6.3. PsychologicalMethodology
7. Competenze in ambito SOC

Per rinforzare la sicurezza aziendale e la consapevolezza degli utenti al problema, creando così una cultura aziendale sul tema, si propone di reiterare le attività attivando un contratto pluriennale, consentendo di ripetere le azioni con una frequenza annuale.Il percorso proposto viene di seguito descritto:



D.R.E.A.M

D.R.E.A.M. è una visione, che pone le sue radici in quello in cui crediamo e si sviluppa attraverso quello che facciamo.

Diagnosis: valutazione della cultura presente

Revelation: condivisione dei risultati

Education: aumento della conoscenza

Action: partecipazione attiva di ciascuno

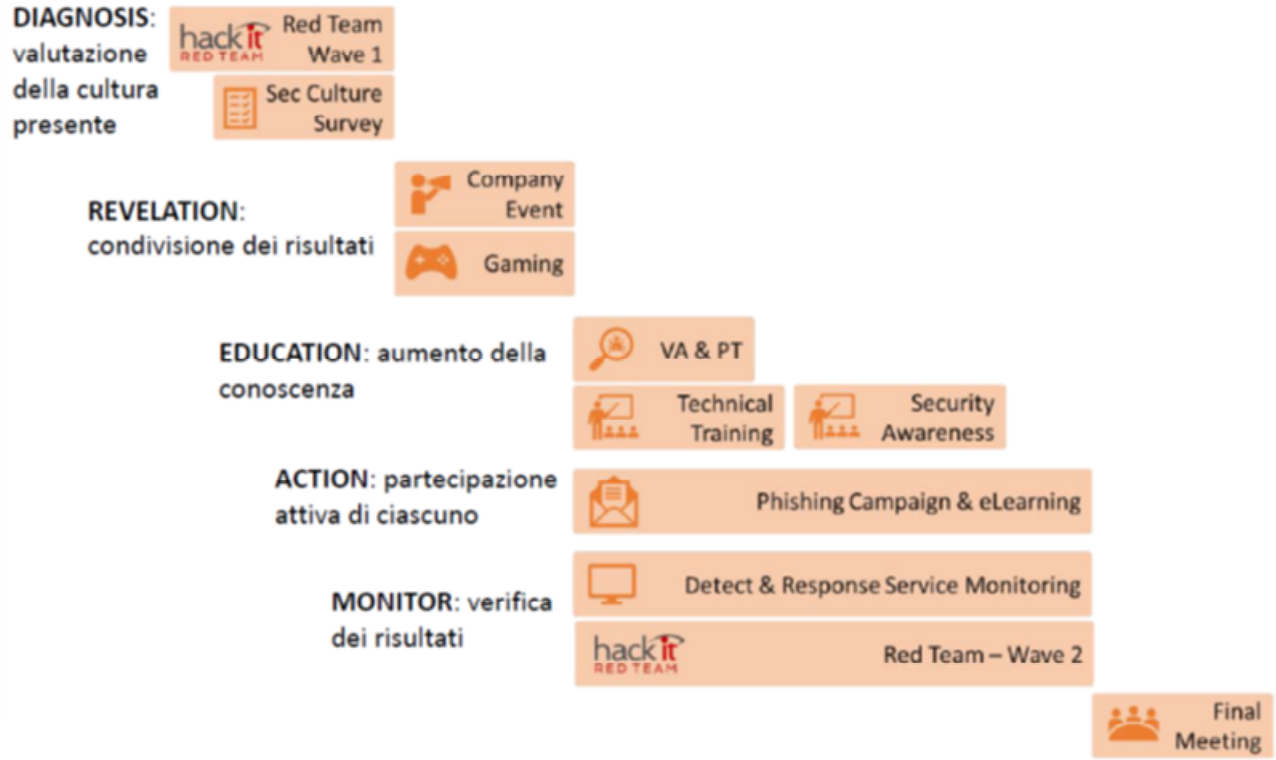
Monitor: verifica dei risultati

2.2.2 Proposta operativa

Lo scopo dei servizi è quello di supportare l'AORN nell'intraprendere un percorso di Trasformazione Culturale per quanto riguarda la Cybersecurity. Tenendo conto della specificità dell'Azienda e utilizzando le nostre competenze ed esperienza si vuole attivare un processo mirato alla costruzione di una visione condivisa da tutta l'Azienda, in relazione ai problemi legati alla sicurezza informatica.

Le attività proposte hanno il fine ultimo di sviluppare una Security Culture aziendale e più precisamente un set di comportamenti che permettano al Gruppo di rilevare e correggere eventuali errori e problemi in una fase iniziale, quando ancora sono risolvibili e non hanno creato un danno all'azienda.

Il percorso proposto viene di seguito descritto nel suo sviluppo temporale, ipotizzando un periodo di un anno, lo schema ha la funzione di rappresentare il flusso logico delle azioni e non è da intendersi come una rappresentazione precisa della durata di ogni singolo momento, per esigenze aziendali è possibile anche rivedere il piano:



2.2.2.1 Diagnosis

Durante questa fase viene effettuata una valutazione della situazione attuale della sicurezza attraverso due metodi distinti per obiettivi:

- Security Culture Survey: è un questionario che serve per mappare le culture presenti in azienda al fine di avere una visione su come la sicurezza viene percepita dalle persone

- Red Team: attraverso una simulazione reale di attacco si evidenzia se e quanto l'azienda è pronta a contrastare un rischio cyber. Il Red Team

RED TEAM – Wave 1

L'infrastruttura IT delle moderne aziende è fatta di sistemi interconnessi tra loro, dove la vulnerabilità di uno può avere effetti a cascata sugli altri. Talvolta queste singole vulnerabilità appaio irrilevanti se viste solo in relazione al sistema che le espone, ma possono risultare molto più gravi se inserite nel contesto più ampio e valutate in base alle conseguenze indirette che queste possono avere anche su altri sistemi o applicazioni.

Lo stesso discorso può essere fatto focalizzandoci sulle persone che compongono l'azienda: si possono investire ingenti somme di denaro in infrastrutture IT di protezione, ma è sufficiente il comportamento errato di un utente per mettere in crisi l'efficacia degli investimenti fatti.

Il nostro servizio di Red Team simula un reale attaccante che sfruttando le vulnerabilità aziendali di un singolo sistema, una piattaforma, un'infrastruttura o una persona, riesce a compromettere la sicurezza dell'intera azienda.

Il nostro approccio olistico, Infrastruttura, Persone e Cultura, incarna il processo mentale degli attuali attaccanti. Esattamente come farebbero gli avversari che utilizzano le più sofisticate tecniche d'attacco, il nostro Red Team esplora tutti gli aspetti della "security posture" aziendale: network Infrastructure, Application Security, Business Processes, Physical Security Control (edificio) e Human Behavior (comportamenti, abitudini, cultura).

A seguito di un'attività di Red Team, avrete una migliore comprensione del livello di sicurezza della vostra organizzazione e saprete dove concentrare i vostri sforzi per migliorarne lo stato.

Il servizio di Red Team proposto vuole dimostrare se e come sia possibile creare un danno di business alle aziende utilizzando mentalità e tecniche offensive reali:un vero attaccante cerca le vulnerabilità più critiche, siano essere tecnologiche o umane, e le usa per raggiungere il proprio scopo, allo stesso modo si comportano gli specialisti.

È anche per questo che la definizione di "perimetro dell'attività", fondamentale per la definizione di un "classico" Penetration Test, assume un significato diverso nel contesto del Red Team. In quest'ultimo caso infatti il "perimetro" è dato dall'azienda stessa e la ricerca del vettore di attacco è parte integrante del servizio.

Per motivi analoghi, il servizio Red Team è un servizio basato sul tempo (3 mesi, 6 mesi, 1 anno) e non sull'estensione dell'infrastruttura, in modo da sapere quanti e quali "danni" riuscirebbe a fare un malintenzionato nel perimetro temporale definito.

La fase definita "OSINT" infatti, ha come obiettivo la raccolta di quante più informazioni possibili sull'azienda, il perimetro tecnologico e le sue persone, al fine di determinare l'approccio più efficacie ed efficiente per strutturale durante le fasi di attacco. Non si tratta pertanto di un'attività esaustiva di analisi delle vulnerabilità, attività, quest'ultima, che ricade sotto il nome di Penetration Test e può essere considerata un'integrazione (complementare) al servizio Red Team.

Sono presenti altri benefici per l'azienda:

DETECTION: Verificare le capacità, da parte della propria infrastruttura di sicurezza o di un servizio SOC, di rilevare un potenziale attacco

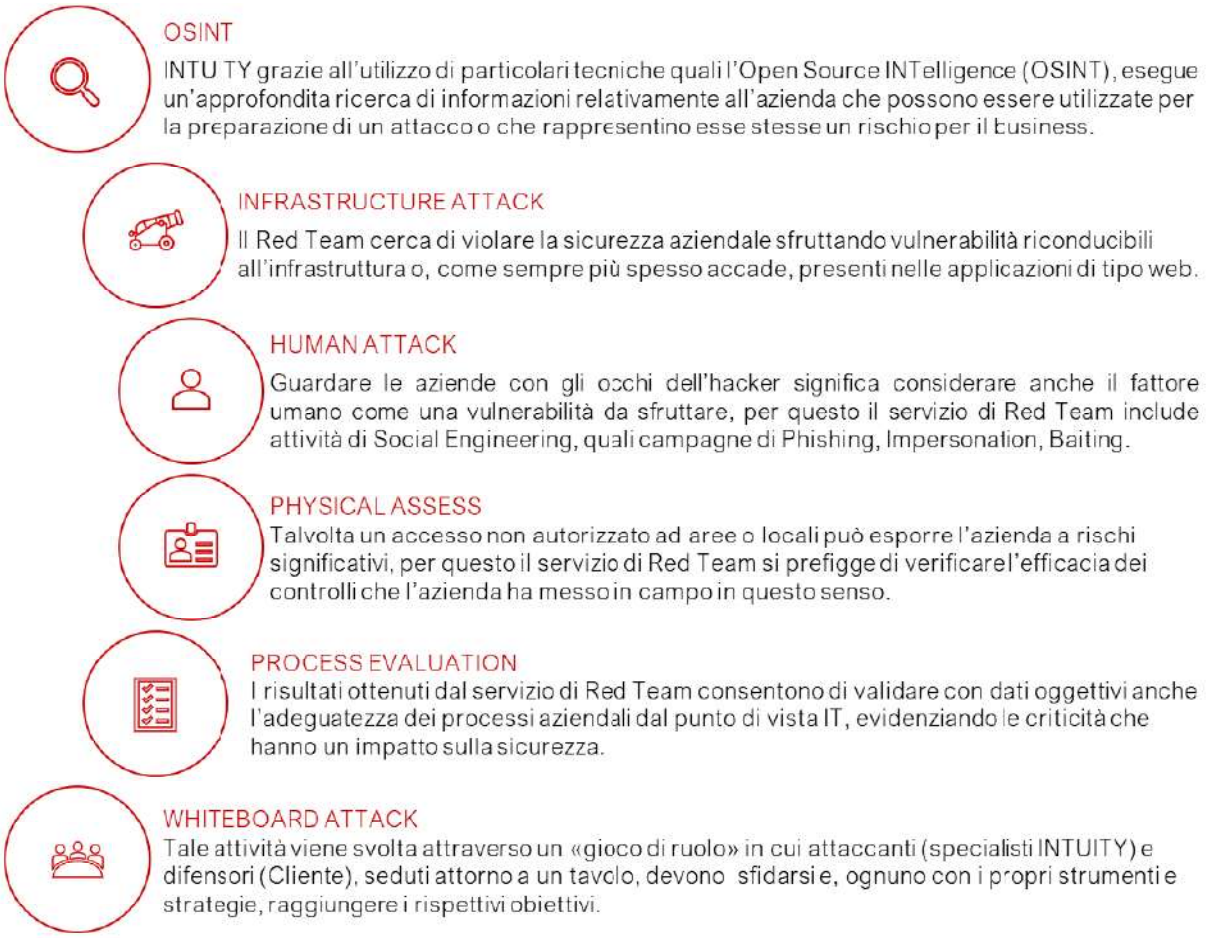
REACTION: Misurare le potenzialità di reazione di fronte a tentativi di intrusione o incidenti di sicurezza.

AWARENESS: Avere una conoscenza più ampia e dettagliata del livello di sicurezza della propria organizzazione.

IMPROVEMENT: Migliorare la propria sicurezza con un piano correttivo basato su evidenze oggettive.

EFFICACY: Scegliere con accuratezza e in modo mirato i propri investimenti di sicurezza.

Le azioni del RED TEAM



RED TEAM – Descrizione Tecnica

Il servizio si compone di attività di Ethical Hacking volte a verificare il livello di sicurezza aziendale. L'obbiettivo del servizio è quello di evidenziare le vulnerabilità infrastrutturali esistenti, eventuali comportamenti non corretti o procedure non correttamente implementare che possano compromettere il business del cliente. Il servizio permetterà di misurare il livello di sicurezza infrastrutturale, il grado di consapevolezza dei problemi di sicurezza da parte dell'azienda, e del livello di Detection& Reaction del cliente rispetto ad attacchi ed incidenti di sicurezza.

Il servizio consente quindi di migliorare l'efficacia della capacità difensiva aziendale e la resistenza agli attacchi sofisticati e persistenti (APT).

Anche se non è possibile definirne a priori i dettagli, in quanto ogni target ha caratteristiche molto diverse dagli altri, il processo d'attacco utilizzato dalla metodologia si basa nel ricercare, catalogare e sfruttare le vulnerabilità aziendali, permettendo d'avere una visione olistica sulla sicurezza delle

applicazioni, del network, del comportamento delle persone che formano l'azienda e quindi della cultura di sicurezza presente.

Red Team si compone di attività che verranno condotte remotamente ed altre presso la struttura target.

La modalità d'attacco prevista è del tipo "BlackBox" che non prevede la condivisione iniziale di informazioni relative al target e alcun tipo di autorizzazione o informazione d'accesso. Questo tipo di modalità permette di "vedere" il target così come lo vedrebbe un attaccante esterno.

L'attacco viene suddiviso in sette fasi principali:

1. ***Goal setting** – Il Cliente, supportato dai nostri specialisti, determina l'obiettivo e le aspettative del servizio di Red Team*
2. ***Reconnaissance**–Red Team, grazie all'utilizzo di particolari tecniche quali l'Open Source Intelligence (OSINT), esegue una approfondita ricerca di informazioni riguardanti i singoli target, con l'obbiettivo di determinare i possibili entry point. L'attività prevede la raccolta di informazioni reperibili pubblicamente che possano risultare utili nella preparazione dell'attacco. Questa fase prevede quindi la raccolta di informazioni reperibili nel dominio pubblico (es. Internet, Forum, Blog, Social Network, …) e presso la struttura target (es. bacheca aziendale). - Attività Remota e On-Site.*
3. ***Infrastructure Attack**– Le informazioni raccolte nella fase precedente vengono utilizzate per condurre attività di Application Attacking, Network Attacking e Wi-Fi Attacking per rilevare le vulnerabilità presenti nell'infrastruttura aziendale. Le attività di Infrastructure Attack verranno condotte analizzando sia il perimetro pubblico (Internet e Wi-Fi) che quello locale (LAN e Wi-Fi). - Attività Remota e On-Site.*
4. ***Social Engineering** – Allo stesso modo, Red Team utilizza tecniche di Social Engineering come il Phishing e l'Impersonation (telefono, chat, …) per ricercare le "Human Vulnerability". Attraverso queste tecniche si cerca ad esempio di indurre le persone a rivelare inconsapevolmente informazioni aziendali confidenziali o comunque che permettano di creare un potenziale danno all'azienda. – Attività Remota e On-Site.*
5. ***Physical Access** – Un altro momento fondamentale del servizio Red Team prevede l'accesso non autorizzato ad ambienti e/o sedi aziendali. Una volta ottenuto l'accesso si cercherà di utilizzare l'infrastruttura interna per effettuare ulteriori attacchi e accedere ad informazioni reperibili localmente quali: documenti abbandonati, password esposte, stampe non ancora ritirate, documenti non adeguatamente stracciati e altro. Questa è la fase definita come: AnthropologicalWalk*
6. ***Exploit &Escalate** – In questa fase, l'Red Team accede al target utilizzando le vulnerabilità scoperte nelle due fasi precedenti: vulnerabilità infrastrutturali, vulnerabilità relative allo "Human Factor" e fisiche. L'attività può quindi includere la manomissione dei processi di business. - Attività Remota e On-Site.*
7. ***Obtain Target** – Sfruttate le vulnerabilità, l'Red Team accede agli asset strategici della struttura target raggiungendo così l'obbiettivo. In questa fase, se necessario, vengono utilizzate tecniche di "LateralMovement": dopo aver compromesso un asset, queste tecniche prevedono di ricercare nuove vulnerabilità che permettano di "muoversi" all'interno della struttura (informatica) con lo scopo di ricercare nuove informazioni di valore. - Attività Remota e On-Site.*
8. ***Remediation** – Al termine dell'esercizio di Red Team, verrà condotta una sessione di presentazione dei risultati con i vari stakeholder aziendali con lo scopo di:*
    - *Rivedere le vulnerabilità riscontrate durante le attività di Red Team*
    - *Presentare i passaggi utilizzati per sfruttare le diverse vulnerabilità, inclusi i "LateralMovement" eseguiti.*
    - *Rispondere a tutte le domande che il team del cliente potrebbe porre relativamente alle vulnerabilità riscontrate e alle attività eseguite.*

- *Discutere degli aspetti strategici relativi alla mitigazione e remediation dei problemi rilevati.*
- *Verificare il grado di "Detection& Reaction" del team di sicurezza aziendale (Blue Team) o del fornitore del cliente, e, nel caso il Blue Team non fosse presente, supportare il cliente nel predisporre tali capacità difensive (Blue Team).*

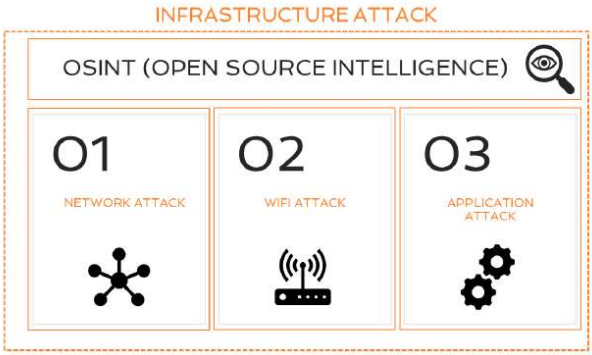
Infrastructure Attack

Le attività previste nel servizio di Infrastructure Attack comprendono:

***Network Attack:** focalizzato a sfruttare le vulnerabilità dell'infrastruttura di sicurezza, networking e sistemistica per verificare come a quanto un attaccante può penetrare in un'azienda attraverso questi mezzi.*

***Wi-Fi Attack**: specificatamente pensato per verificare la sicurezza di una rete Wi-Fi attraverso attacchi specifici.*

***Web Application Attack**: volta a sfruttare le vulnerabilità delle applicazioni web che sempre più spesso rappresentano un veicolo per penetrare in un'azienda, arrecarle danni o sfruttarla per portare attacchi verso terzi.*



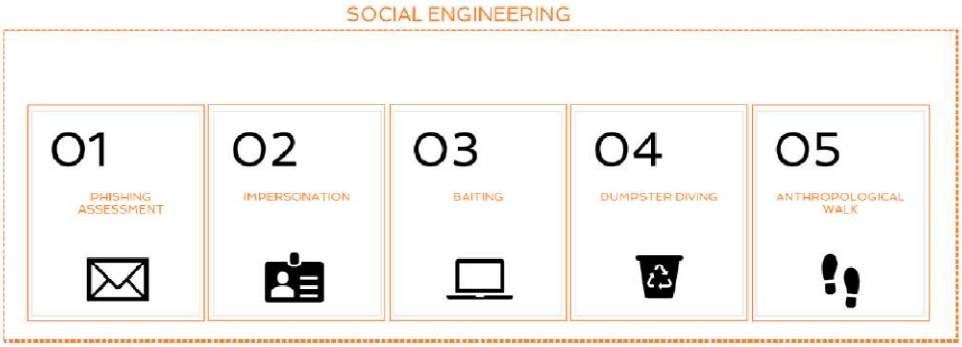
Social Engineering

Come sopra riportato, il servizio RED TEAM prevede di simulare una serie di attacchi agli utenti aziendali attraverso attività di tipo Social Engineering che, grazie alla rilevazione dei comportamenti degli utenti, permettano di misurare il livello di Security Awareness aziendale.

Per raggiungere tale scopo, verranno effettuati una serie di attacchi simulati (Impersonation, Phishing, Baiting, …). I risultati degli attacchi verranno condivisi con il cliente al fine di sviluppare una serie di remediation che vadano a risolvere le vulnerabilità rilevate.

Il servizio di RED TEAM prevede la possibilità di simulare attacchi che, sfruttando le vulnerabilità dell'umano (Cognitive Biases) possano permettere l'accesso fisico ai locali del target.

Di seguito vengono descritte le diverse fasi proposte.



Phishing: *uno dei principali veicoli di attacco ai giorni nostri è rappresentato dall'email, per questo una delle azioni principali del Social Engineering è rappresentato da una o più campagne di phishing finalizzati ad ottenere credenziali utilizzabili, veicolare malware all'interno della rete aziendale o guadagnare accesso ad un dispositivo mobile (Android o iOS)*

Impersonation*: Questa attività prevede l'impersonificazione di identità da parte di specialisti.*

Allo scopo di rendere credibili tali identità, il team eseguirà delle azioni di Information Gathering attraverso le tecniche OSINT. Verranno quindi simulate le identità di colleghi, fornitori o di clienti allo scopo di ottenere informazioni utili per accedere a sistemi o dati sensibili del cliente.

L'obiettivo di questa attività è di evidenziare vulnerabilità nei processi aziendali nella gestione delle informazioni sensibili.

Baiting: *Le attività di Baiting fanno leva sulle debolezze tipiche dell'essere umano quali: curiosità, distrazione, mancanza di attenzione o di consapevolezza.*

Il servizio prevede di distribuire in maniera pseudo casuale delle chiavi USB all'interno o all'esterno del perimetro aziendale, simulando uno smarrimento.

La chiave USB contiene un contenuto malevolo controllato che si attiva al momento dell'apertura.

L'attacco prevede di posizionare alcune chiavette USB compromesse all'interno di un'area precedentemente scelta dal cliente.

DumpsterDiving: *Il DumpsterDiving è una tecnica utilizzata per recuperare dai rifiuti aziendali informazioni utili alla pianificazione e alla riuscita di un attacco informatico. I dati ricercati non sono soltanto le credenziali di accesso scritte in un foglietto, ma anche documentazione classificata (Internal/Confidential) o informazioni apparentemente innocenti che possono essere sfruttate in attività di Social Engineering.*

Questa tipologia di attacco non ha soltanto l'obiettivo di compromettere la sicurezza aziendale, ma può creare un danno reputazionale alla stessa.

AnthropologicalWalk: *L'AnthropologicalWalk è un'attività che ha lo scopo di raccogliere e classificare informazioni ottenute grazie ad una ricerca sul campo mediante osservazione e ascolto.*

L'obiettivo dell'attività è di effettuare un'analisi comportamentale, senza portare alcun attacco.

Ad esempio, a quali informazioni un consulente potrebbe accedere durante l'attività lavorativa semplicemente spostandosi di ufficio, camminando per i corridoi, entrando in aree sguarnite o sfruttando la connettività che gli viene fornita.

L'attività prevede di accedere in area aziendale come consulente o guest e con tutti i privilegi previsti (es. connettività, aree di accesso, etc.).

<u>RED TEAM – Reportistica</u>

Al termine del servizio e mensilmente per un'attività di durata annuale, verrà fornita e discussa tutta la documentazione contenente le informazioni rilevanti ottenute.

La reportistica fornita sarà di due tipi, uno di tipo Executive (ppt) e uno Tecnico (pdf).

Executive Report, che riassume ad alto livello i risultati delle analisi, focalizzandosi sui principali rischi identificati e fornendo una visione d'insieme del livello di sicurezza di quanto analizzato.

Technical Report, che riassume i risultati delle analisi, dettagliandone gli aspetti tecnici e le modalità di riproduzione, e definendo le misure per correggere le problematiche identificate.

Perimetro per attività di "RED TEAM"

- *Tipologia di attività: RED TEAM*
  - *OSINT*
  - *IT Infrastructure Attack – Servizi pubblicati e servizi interni sul perimetro IP relativo al cliente*
  - *Social Engineering Attack (Phishing, Impersonation, Bating, etc.) sui dipendenti del cliente*
  - *Physical Access: Test sulla sede di Napoli (Accesso struttura e locali, accesso PC e sistemi incustoditi)*
- *Obbiettivo: Verifica dei rischi cyber e fisici con particolare focalizzazione ai dati sensibili.*
- *Metodologia: BlackBox – il team non avrà a disposizione alcuna informazione da parte del cliente.*
- *Hacking Point of View – Public & Private space*
- *Durata dell'attacco – 2 mesi*
- *Reportistica discussa al termine dell'attività.*

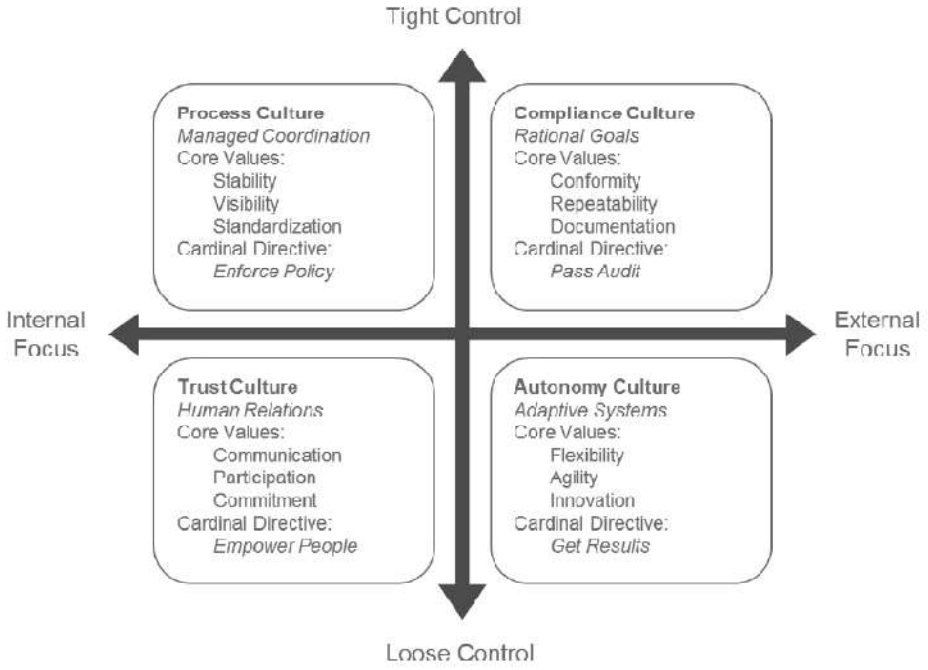
Nel caso in cui, durante l'attività, il team venisse a conoscenza di informazioni sensibili o situazioni particolarmente critiche, ne verrà data immediata conoscenza alle persone indicate dal cliente.

Security Culture Survey

L'obiettivo di questa Survey è di mappare le diverse culture presenti in azienda, ossia capire come persone diverse e team diversi percepiscono il tema della sicurezza informatica.

Si tratta di un questionario di 10 domande, ognuna di queste ha 4 diverse risposte alle quali il rispondente deve attribuire un valore di importanza.

Il risultato finale è un prospetto che identifica quali e quanto dei seguenti atteggiamenti nei confronti della sicurezza è presente in azienda:



2.2.2.2 Revelation

La proposta per questa fase è di creare un momento di condivisione, idealmente di mezza giornata, durante la quale l'azienda con la nostra guida si immergerà nel tema della Cybersecurity attraverso 4 momenti estremamente coinvolgenti:

1) Panorama sul mondo della sicurezza informatica, dati e casi reali
2) Gioco di ruolo "Catch it, ifyou can" (vedi paragrafo 6.1)
3) Esposizione dei risultati della Fase 1 – Diagnose
4) How to hack a Smartphone: dimostrazionepratica

Game "Catch it, if you can"

In questo gioco le varie squadre rappresentano il "reparto information security" di un'azienda e devono capire come possa essere avvenuto un data breach (un file riservato è finito fuori dall'azienda) analizzando l'ufficio di un dirigente. L'obiettivo è costringere i partecipanti ad analizzare una situazione e comparare quello che vedono con quello che sanno per identificare situazioni di rischio.

La scrivania sarà organizzata in modo da contenere 10 situazioni di rischio.

Punti

- *Chi fornisce una spiegazione pratica di come il file possa essere stato trafugato: 5 punti*
- *Ogni indizio trovato: 1 punto*
- *Chi trova tutte e 10 le situazioni di rischio: 4 punti aggiuntivi*
- *Chi trova e motiva una situazione di rischio diversa dalle 10 predefinite: 2 punti*
- *Chi esegue il file .exe dalla chiavetta USB: -2 punti*

Svolgimento

Al via ogni squadra si recherà presso la propria "scrivania" ed inizierà l'analisi, un membro della squadra sarà nominato "Analyst" e dovrà scrivere quanto viene rilevato ed esporlo in seguito. Ci saranno 20 minuti per analizzare la scrivania, 10 per organizzare i risultati e 5 minuti a squadra per esporli. Gli indizi che si potranno trovare presso la scrivania saranno (indicativamente):

- *Il notebook non è bloccato*
- *Aprendo il client di posta si trovano, tra le altre:*
  - *una mail di phishing inviata da un sedicente "manager" chiedendo che gli fosse inviato il file riservato*
  - *nella posta in uscita c'è la risposta con il file allegato (DATA BREACH)*
  - *sempre tra la posta inviata c'è una e-mail con la quale il dirigente invia al suo indirizzo di posta privato il file riservato*
  - *diverse e-mail di pubblicità e newsletter personali, segno che il dirigente ha usato il suo account aziendale per iscriversi a portali ad uso personale*
- *La chiavetta USB sopra la scrivania contiene un file di tipo .exe*
  - *In questo caso l'indizio è rappresentato dal file .exe, ma se qualcuno degli analisti lancia l'eseguibile perde 2 punti perché mette esso stesso a rischio l'azienda.*
- *Sul desktop del PC c'è una cartella protetta da password "dati riservati", ma la password di quella stessa cartella di trova annotata in un post-it sotto al PC*
- *Sopra la scrivania ci sono diversi documenti sensibili*
- *Dentro al cestino si trova parzialmente stracciato, ma ancora leggibile una mail stampata con la quale venivano comunicate la username e password per accedere ad un portale interno con dati sensibili e l'invito a modificare la password al primo accesso*

- *Sul desktop è presente un link al portale al quale ancora si accede con username e password scritte sul documento trovato nel cestino (ad indicare che non sono mai state cambiate)*

2.2.2.3 Education

Durante questa fase si vogliono fornire competenze utili alle persone per fronteggiare il problema della cyber security. Sono proposte attività formativa diverse per tipologia di utente a seconda del ruolo.

Anche in questo caso l'obiettivo è creare momenti quanto più coinvolgenti possibile.

Security Awareness Training

Scopo del servizio è quello di rendere consapevoli utenti del cliente delle problematiche legate alla cybersecurity. Il servizio prevede sessioni di training da tenersi in aula con un esperto della materia presso gli uffici del cliente ed avrà una durata per singola sessione di massimo 3 ore. Ogni sessione sarà composta da un numero consigliato di 30 persone.

Gli argomenti trattati sono elencati di seguito in maniera non esaustiva:

- *Come funziona Internet, cosa significa essere "connessi".*
- *Web, cos'è, quali sono i pericoli che nasconde, come riconoscerli ed evitarli.*
- *E-mail, cos'è, perché è diventata il primo veicolo di attacco, cos'è il Phishing e come riconoscerlo.*
- *Strumenti mobili, laptop e Smart device, sono l'azienda fuori dall'azienda, come usarli in modo sicuro, come evitare di esporre sé stessi e l'azienda a furti di dati ed informazioni.*
- *Social Network, una quantità immane di informazioni a disposizione di tutti, come evitare di esporre sé stessi e l'azienda a rischi inutili.*

Il contenuto del training verrà comunque condiviso e discusso con il personale del cliente e comunque a seguito della presentazione dei risultati dell'attività di RED TEAM.

Technical Security Training

Questa serie di training è rivolta agli utenti più tecnici ed ha l'obiettivo di fornire competenze sulla sicurezza informatica.

Per rendere i training più pratici e coinvolgenti saranno utilizzate, come basi per la formazione, dei casi pratici che TIM ha visto, vissuto ed analizzato, oltre che esercitazioni pratiche. Ripercorrendo i passi effettuati durante gli attacchi presi in esame si andranno così ad approfondire i concetti teorici:

Prima sessione di training, 1 giorno:

- *Security Best Practice, quali sono rispetto a modelli di riferimento come CIS e ISO27001*
- *Perché è opportuno seguire le Best Practice*
- *Caso reale di attacco e come le Best Practice avrebbero mitigato il problema*

Seconda sessione di training, 1 giorno:

- *Analisi di altri casi reali*
- *Fasi dell'attacco*
- *Applicazione delle Best Practice in casi reali*

Terza sessione di training (White Board Attack), 0,5 giorni:

- *La Whiteboard Attack Simulation è un'attività del tipo "Gioco di Ruolo" tra gli specialisti ed il personale del cliente. L'attività prevede la simulazione di attacchi portati in maniera teorica, senza*

quindi un impatto sull'operation aziendale. Lo scopo è di verificare la capacità di "Detection& Reaction" aziendale a seguito delle diverse ipotesi di attacco proposte dagli specialisti.

Phishing Campaign& eLearning

Per rinforzare il messaggio di consapevolezza e tenere alto il livello di attenzione al problema, trasformando il comportamento dell'utente in abitudine, viene erogato il servizio di Phishing Campaign. Lo scopo è di raggiungere il più elevato numero di utenti possibile utilizzando mail dal contenuto generico, per verificare quanto essi siano in grado di riconoscere una minaccia veicolata in questo modo.

L'attività Phishing Campaign è così dimensionata:

- *L'attività proposta si focalizza su tutti gli utenti del cliente.*
- *Tipologia di mail inviate: Malicious Link e Malicious Attachment.*
- *Numero mail recapitate per singola mailbox: 1 al mese.*
- *Durata dell'intera campagna: 10 mesi (indicativamente).*

Il servizio viene erogato in modalità continuativa con lo scopo di mantenere elevata l'attenzione sul problema del Phishing. Inoltre, sempre per migliorare la consapevolezza degli utenti per quanto concerne le tematiche di CyberSecurity, si attuano azioni formative veicolate attraverso microtraining. In particolare, a seguito di una mail di Phishing inviata dal sistema di sicurezza, l'utente che apre il link o l'allegato contenuto nella mail, viene automaticamente reindirizzato verso il contenuto desiderato: pillole informative, quiz, esercizi interattivi.

I risultati dell'attività saranno analizzati dal team e presentati in un report, per poi essere condivisi e discussi con il cliente al fine di definire le opportune attività correttive.

Policy & Procedure Review

Policy e procedure, se scritte con ragionevolezza, hanno la funzione di guidare le persone verso comportamenti che siano costruttivi per l'azienda, questo è l'obiettivo da raggiungere.

Con il supporto di TIM, grazie all'attività condotta quotidianamente e grazie ai risultati ottenuti nelle fasi precedenti, si attiverà un processo (se non già esistente) che porti alla revisione continua di processi e procedure aziendali.

2.2.2.4 Monitor

Quest'ultima fase ha un duplice obiettivo: monitorare l'efficacia delle azioni intraprese durante le altre fasi attraverso il metodo empirico del Red Team, contestualmente si rilevano altre situazioni di rischio per l'azienda, che saranno condivise ed analizzate durante le sessioni di training e nel corso del meeting finale.

RED TEAM Continuous Wave - Perimetro

- *Tipologia di attività: RED TEAM*
  - ✓ *OSINT*
  - ✓ *IT Infrastructure Attack – Servizipubblicati*
  - ✓ *Social Engineering Attack (Phishing, Impersonification, Bating, etc.)*
  - ✓ *Physical Access: Test su due sedi/impianti a scelta (Accesso struttura e locali, accesso PC e sistemi incustoditi)*
- *Obbiettivo: da definire con il Gruppo.*
- *Metodologia: BlackBox – il teamnon avrà a disposizione alcuna informazione da parte del cliente.*
- *Hacking Point of View – Public & Private space*
- *Durata dell'attacco – 8 mesi*

- *Reportistica discussa al termine dell'attività.*

Nel caso in cui, durante l'attività, il team venisse a conoscenza di informazioni sensibili o situazioni particolarmente critiche, ne verrà data immediata conoscenza alle persone indicate dal cliente.

Final meeting

Idealmente questo è un momento finale durante il quale si condivide con tutta l'Azienda il risultato delle azioni intraprese, si analizzano i problemi riscontrati e se ritenuto opportuno si possono premiare simbolicamente i "cyber security heroes", persone che hanno avuto un atteggiamento esemplare e costruttivo nei confronti della sicurezza aziendale: chi ha segnalato situazioni di criticità ad esempio.

Qual ora fosse difficoltoso organizzare un ulteriore meeting aziendale è possibile realizzare un momento di condivisione con un webinar.

Detect&Response Service Monitoring

Il servizio Blue Team – Detect&Response Service, composto da Security Specialist è parte della suite Blue Team, una serie di servizi estremamente integrati tra loro che attraverso La Detection, Reaction e Prevention, ha come missione difendere le aziende dalle diverse minacce presenti e future. La suite Blue Team sposa il concetto di People Centric Security mettendo al centro delle proprie attenzioni l'utente aziendale, e quindi il business dell'organizzazione.

In particolare, il servizio Blue Team – Detect&Response Service ha come caratteristica il controllo costante, rilevando ed investigando le minacce nelle prime fasi dell'attacco (Attack Chain), bloccandolo prima che questo possa mettere in crisi il business aziendale.

Gli specialisti, grazie alla loro esperienza e competenza e all'utilizzo di strumenti professionali (RAPID 7 Insight IDR), sono in grado di rilevare le minacce grazie a tecniche particolari e a sistemi di alerting molto efficaci, riuscendo a focalizzarsi sulle attività anomale e sospette ed eseguendo attività di AnomalyDetection e User Behaviour Analysis.

Il servizio Blue Team – Detect&Response Service ha lo scopo di proteggere il business dell'azienda e lo raggiunge focalizzandosi su due principali obbiettivi:

1. *Proteggere i dati aziendali*
2. *Proteggere gli utenti*

Protezione dei dati

Il servizio monitora costantemente le attività di autenticazione rilevando in tempo reale gli accessi ai sistemi sensibili e strategici per la sicurezza aziendale. Gli specialisti configureranno i propri strumenti in modo da distinguere gli utenti inseriti precedentemente in white o black list. Questo permette di identificare gli accessi non autorizzati e quindi minacce interne e/o esterne. Inoltre, grazie a questi controlli gli specialisti possono proporre al cliente l'ottimizzazione delle policy di sicurezza dell'infrastruttura aziendale.

Protezione degli utenti

Il servizio Blue Team, Detect&Response Service, come tutti i servizi previsti, mette l'utente al centro del processo di sicurezza. In particolare, il servizio si focalizza sul monitoraggio degli account degli utenti: i principali target degli attacchi sofisticati. Il servizio è in grado di analizzare e correlare gli account utenti con gli asset utilizzati, la network activity eseguita e qualsiasi dato rilevato dall'infrastruttura di sicurezza aziendale, monitorando le attività anomale e gli indicatori di compromissione. In questo modo, gli specialisti, hanno una fotografia più completa, guardando non solo cosa è coinvolto ma chi ne è

responsabile, quando l'evento è accaduto e prevenendo le prossime mosse dell'attaccante. In questo modo è possibile analizzare qualsiasi comportamento anomalo degli utenti per identificare eventuali intruder rilevando credenziali compromesse, lateralmovement e altre tipologie d'attacco.

Il servizio, erogato remotamente, si basa su un Collector da inserire all'interno del network aziendale che ha il compito di raccogliere gli eventi rilevati dai diversi componenti infrastrutturali dell'azienda:

- *Active Directory*
- *Firewall*
- *LDAP*
- *E-mail Server*
- *DHCP*
- *Security Console*
- *DNS*
- *Enterprise Cloud Application (es. O365, Salesforce, …)*
- *VPN*
- *Intruder Traps (Honeypot)*
- *IDS/IPS*
- *End-Point (client)*
- *Web Proxy*
- *Mobile*

Il Collector raccoglie i dati/log dalle diverse fonti sopramenzionate. I dati vengono aggregati dal Collector filtrando i dati sensibili (es. i dati personali) ed inviando le informazioni utili in maniere sicura nel Cloud che ospita la piattaforma.

Il servizio è erogato tutti i giorni lavorativi dal lunedì al venerdì dalle 8:30 alle 18:30 in modalità proattiva e in modalità reattiva gli altri giorni/orari.

Il servizio è dimensionato per il monitoraggio e raccolta di eventi in base al numero di asset (circa 2000).

<u>VulnerabilityAssessment e Penetration Test</u>

Scopo di questa attività è quello di evidenziare e supportare il cliente nel correggere le vulnerabilità presenti nell'infrastruttura aziendale, a livello network, sistemistico ed applicativo.

Le attività di Assessment non riguarderanno solo l'infrastruttura aziendali ma anche i servizi e le applicazioni rese disponibili ai propri clienti.

Tale servizio, garantito dal team, si compone delle seguenti attività:

1. *Esecuzione delle attività di VA-PT*
2. *Discussione con il cliente dei risultati del test e Remediation Plan*
3. *Supporto nell'implementazione del Remediation Plan*
4. *Ripetizione del test di VAPT per la verifica della corretta implementazione delle contromisure*
5. *Discussione con il cliente dei risultati del test*

L'attività consiste nel simulare una serie di attacchi verso l'infrastruttura aziendale, pubblica e privata; tali test hanno la finalità di evidenziare le vulnerabilità sia a livello applicativo che sistemistico e di verificare quali tra queste possano essere realmente sfruttate descrivendone quindi il metodo di attacco. Tale attività permette di poter verificare tra l'altro la qualità delle remediation applicate.

L'attività si sviluppa nelle seguenti 6 fasi:

1. ***Information Gathering** - Analisi di tipo Open Source Intelligence (OSINT) con l'obbiettivo di determinare i possibili entry point delle applicazioni. L'attività prevede la raccolta di informazioni reperibili pubblicamente che possano risultare utili nella preparazione dell'attacco.*
2. ***System VA** - Al fine di includere tutti i vettori d'attacco sfruttabili da un hacker nei confronti dei sistemi, viene inclusa nell'analisi un'attività di VulnerabilityAssessment a livello sistemistico infrastrutturale, includendo quindi le piattaforme che ospitano le applicazioni aziendali.*
3. ***Application VA** - L'attività inizierà con una scansione BlackBox per ricostruire la struttura di ogni singola applicazione e rilevarne vulnerabilità a livello applicativo, quali ma non solo: SQL Injection, XSS, etc. Saranno effettuati controlli per tutte le vulnerabilità rilevabili con particolare enfasi per le Top 10 OWASP. Tra le applicazioni analizzate includiamo anche le Mobile App in ambiente iOS, Android e Windows Mobile.*
4. ***Analysis** - Le vulnerabilità riscontrate durante le tre fasi precedenti, OSINT, System VA e Application VA verranno raccolte, catalogate ed analizzate al fine di pianificare l'attività di Exploitation.In questa fase saranno validate le vulnerabilità riscontrate per determinare i possibili vettori di attacco. Sarà inoltre definito un piano di attacco che distingua quali vulnerabilità possano essere sfruttate in modalità BlackBox (non autenticata) e quali in modalità WhiteBox (autenticata).Qualora si rilevi un potenziale rischio di impatto sul servizio erogato dall'applicazione, verrà condiviso con il cliente un piano di esecuzione.*
5. ***Exploitation -** La fase di Exploitation di un Penetration Test si focalizza esclusivamente sull'ottenere accesso ad un sistema o una risorsa eludendo eventuali controlli di sicurezza. Questa fase deve essere pianificata con attenzione per essere efficace, sfruttando appieno i risultati delle fasi precedenti. Verrà quindi verificato se le vulnerabilità riscontrate siano realmente sfruttabili, facendo uso di "exploit code" disponibile pubblicamente, strumenti professionali di Penetration Test e personalizzando il codice di Exploitation. L'attività di Exploitation (Penetration Test), verrà discussa precedentemente con il personale dell'azienda e comunque suggerita ogniqualvolta il cliente o lo specialista lo ritenga necessario.*
6. ***Reporting** - Al termine delle attività di Exploitation, verrà fornita e discussa tutta la documentazione contenente le informazioni rilevati ottenute durante tutte le fasi del processo.*

<u>Supporto implementazione Remediation</u>

Il team a disposizione del cliente supporterà l'azienda nell'implementazione delle remediation relative alle vulnerabilità riscontrate. Tale attività consiste nella consulenza nell'implementazione di azioni correttive infrastrutturali, sistemistiche ed applicative che possano risolvere le vulnerabilità riscontrate. Come esempio, tra le soluzioni proposte possiamo includere l'implementazione di aggiornamenti applicativi, la modifica delle policy di sicurezza, l'implementazione di nuove soluzioni applicative e/o tecnologiche.

<u>Monitoraggio Vulnerabilità</u>

Grazie alla piattaforma di Vulnerability Management (vedi par. 12), gli specialisti INUTITY saranno in grado di monitorare le vulnerabilità presenti nei singoli componenti dell'infrastruttura del Gruppo. I

risultati di ogni scansione effettuata verranno storicizzati dalla piattaforma di Vulnerability Management in modo da poter verificare l'andamento delle vulnerabilità per ogni singolo componente infrastrutturale nel tempo.

Tale attività permette di poter verificare tra l'altro la qualità delle remediation applicate.

Perimetro

Le attività di VulnerabilityAssessment e Penetration Test, Tipologia di attività: Network & WEB Application Penetration Test

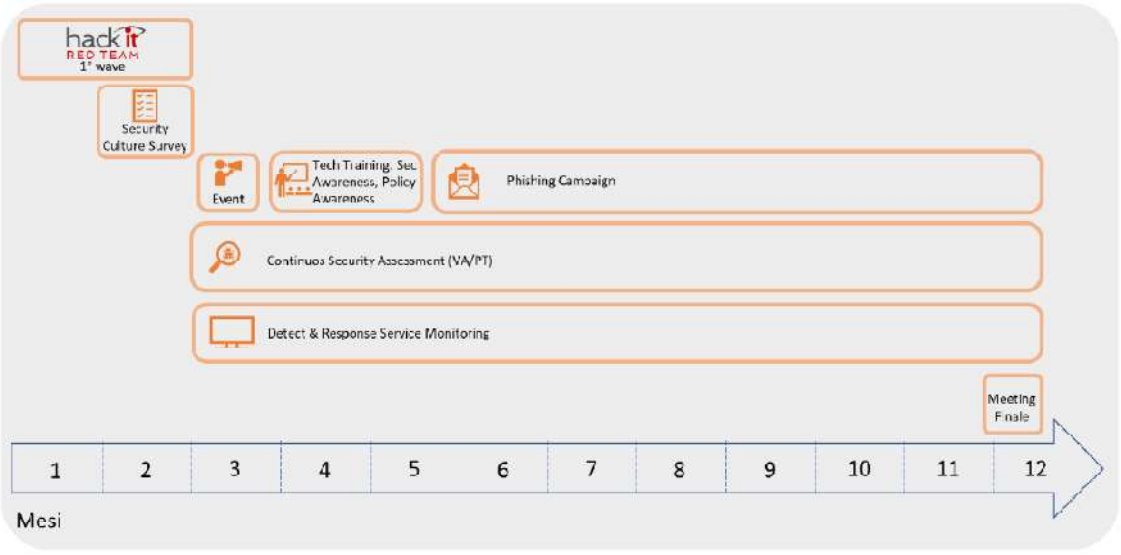
- *Target: Infrastruttura ed applicazioni aziendali e applicazioni sviluppate internamente*
- *Metodologia: BlackBox (senza credenziali) e GreyBox (condivisione di credenziali "utente")*
- *Hacking Point of View: Internet e Intranet*
- *Frequenza: Ogni singola applicazione verrà sottoposta ad una seconda analisi a seguito dell'implementazioni delle eventuali remediation*
- *Durata del servizio: Annuale – Servizio continuativo*

Trattandosi di servizio "continuativo" la reportistica (tecnica e/o executive) verrà redatta quando l'azienda lo riterrà necessario (audit, richiesta cliente, richiesta interna, …).

Le attività di rilevazione delle vulnerabilità (scansione) dell'intera infrastruttura del Gruppo potrà essere condotta e quindi richiesta dal personale un numero illimitato di volte e per un numero illimitato di Web Application. Sarà comunque compito dello specialista suggerire e proporre tale attività ogniqualvolta lo ritiene necessario.

2.2.3 Stima temporale

1. Anno



2. Anno


hack it
RED TEAM
2° wave
Security Culture Survey
Event
Tech Training, Sec Awareness, Policy Awareness
Phishing Campaign
Continuos Security Assessment (VA/PT)
Detect & Response Service Monitoring
Meeting Finale
1
2
3
4
5
6
7
8
9
10
11
12
Mesi